UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/805,279	03/13/2001	Robert M. Barnhart	SAIC0039	1264

27510 7590 06/13/2007
KILPATRICK STOCKTON LLP
607 14TH STREET, N.W.
WASHINGTON, DC 20005

EXAMINER	
JARRETT, SCOTT L	

ART UNIT	PAPER NUMBER
3623	

MAIL DATE	DELIVERY MODE
06/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/805,279	BARNHART, ROBERT M.	
	Examiner	Art Unit	
	Scott L. Jarrett	3623	

. -- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *29-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 April 2007* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This **Final** Office Action is in response to Applicant's Amendments filed April 6, 2007. Applicant's amendments amended the Specification, Drawings, and Abstract. Currently Claims 29-33 are pending, claims 1-28 being previously canceled.

Response to Arguments

2. Applicant's arguments filed April 6, 2007 have been fully considered but they are not persuasive. Specifically Applicant's argue that

- the examiner has mischaracterized the claim language ("The Final OA mischaracterizes the claim language, with the effect that the claims as submitted by the applicant, have not yet been examined. Mischaracterized terms include "cast ballots," "vote serial number," and "user.", Remarks: Bullets, Page 7);
    - "The OA mischaracterizes SHRADER and CRANOR to find a non-existent "user" in those references." (Remarks: Bullets, Page 7);
    - substituting "ballot" (e.g., a list of candidates for each position in an election) for "cast ballot" (Bcast, which includes voter's choices); (Remarks: Bullets, Page 15);
    - substituting "voter' s identification number" and" ballot number" for "vote serial number (VSN)"; (Remarks: Bullets, Page 15); and
    - substituting "entity, ... system, subsystem, third party" for "user;" (Remarks: Bullets, Page 15);

- the prior art of record fails to teach or suggest each and every element of the claimed invention:
  - "SHRADER discloses the wrong data, encrypted with the wrong key." (Remarks: Bullets, Page 7);
  - "neglecting to account for the inclusion of the digital signature of the cast ballot using the server's private key as an element of the association called for in Claim 31." (Remarks: Bullets, Page 15).

In response to Applicant's argument that the Non-Final Office Action mailed December 7, 2006 mischaracterizes the claim language the examiner respectfully disagrees.

As an initial matter the examiner has given the terms cast ballot, vote serial number and user the usual and customary definitions (cast ballot: voted ballot, committed ballot, vote, completed ballot, submitted ballot, vote; vote serial number: any unique vote identifier). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Specifically, in response to the Applicant's argument that the OA mischaracterized the phrase "cast ballot" the examiner notes that the prior art of record clearly teaches voters casting (submitting) their ballots wherein the ballots (vote) contains their choices and further wherein those cast ballots are commonly protected by

some a cryptographic function such as a digital signature, PKD encryption or the like (Shrader et al.: Paragraphs 0048-0053).

Shrader et al. teach a system and method for securely voting over a network wherein voters complete and submit (cast) their ballots (Paragraphs 0035, 0041, 0042, 0059-0060; Figure 4, Elements 44-45; Figure 7, Elements 66-67).

> "*Voting entity casts its votes and encrypts the votes and the electronic ballot* with the public key of the voting tabulator before sending the encrypted voting information to the voting tabulator.", emphasis added, Paragraph 0062

Cranor et al. teaches a system and method for securely voting over a network wherein users (voters) cast and sign (encrypting, sealing) their cast ballot (encrypted ballot; Paragraph 5, Page 7; Paragraph 3, Page 8; Figure 1, b - blinded ballot digest).

> Pollster The pollster acts as a voter's agent, presenting human readable ballots to a voter, *collecting the voter's responses to ballot questions, performing cryptographic functions* on the voter's behalf, obtaining necessary validations and *receipts, and delivering ballots to the ballot box.* (emphasis added, Paragraph 5, Page 7)
>
> Tallier The tallier is responsible for *collecting the voted ballots* and tallying the results of the election or survey. *Voters first submit encrypted ballots, signed by the validator to the tallier.* The tallier checks the authenticity of the validation and verifies that the *encrypted ballot is unique* among the encrypted ballots received thus far. If the ballot is valid and unique, the tallier *issues a signed receipt to the voter.* The voter then submits the ballot decryption key. The tallier uses the key to

> decrypt the ballot. After the election, the tallier publishes a list of encrypted ballots, decryption keys, and decrypted ballots, allowing for independent verification of election results. (emphasis added, Paragraph 3, Page 8)

Specifically, in response to the Applicant's argument that the OA mischaracterized the phrase "vote serial number", as defined by the specification "Note that the VSN... is ***just an incidental sequence number*** that indicates a vote was delivered in the election" (emphasis added, Paragraph 0054), the examiner respectfully disagrees.

Shrader et al. teach a system and method for securely voting over a network wherein ballots, both cast and pre-cast, are assigned a vote serial number (unique identifier; Figure 6, Element 58; ballot number, Paragraph 0063;

> "creates a electronic ballot consisting of the unique election identification and *ballot serial number*", emphasis added, Paragraph 0061

Cranor et al., teaches a system and method for voting securely over a network comprising associating at least two unique identifiers to ballots cast by voters wherein the unique identifiers (vote serial numbers) are generated and associated with the cast ballot only *after* the voters casts their ballot containing their choices (receipt number: Paragraphs 3-4, Page 8; Figure 1; index number for uniquely identifying, accessing and storing cast ballots in a database, Paragraph 4, Page 8)

> Our tallier computes a 16-byte digest of *each encrypted ballot received* and uses it *to index the encrypted ballots and receipts*. A hash table could be added for greater efficiency in *looking up encrypted ballots*. This modification is probably

necessary to accommodate large-scale elections. (emphasis added, Paragraph 4, Page 8)

Specifically, in response to the Applicant's argument that the OA mischaracterized the phrase "user" the examiner respectfully disagrees.

Shrader et al. teach a system and method for secure network voting wherein at least one of the system/method participants/users is a voter who casts a ballot (Paragraphs 0035, 0041, 0042, 0059-0060; Figure 4, Elements 44-45; Figure 7, Elements 66-67).

Cranor et al. teach a system and method for securely voting over a network wherein at least one of the system/method participants/users is a voter who casts a ballot (Paragraph 5, Page 7; Paragraph 3, Page 8; Figure 1).

Additionally it is noted that the invention as claimed merely recites "making a confirmation token available to *a user*" wherein the claim does not positively recite that the "a user" performs any of the method steps as claimed nor does the invention as claimed positively recite which user (the "a user" recited in the preamble or another user of the system) the token is made available to nor does the invention as claimed positively recite what entity (the "a user" in the preamble or some other entity/participant) actually retrieves/receives the now available confirmation token nor does the invention as claimed positively recite what entity performs the comparison to determine that the cast ballot is verified (the "a user" of the preamble or another method participant/entity).

In response to Applicant's argument that the prior art of record fails to teach or suggest each and every element of the claimed invention the examiner respectfully disagrees.

Specifically regarding Applicant's argument that "SHRADER discloses the wrong data, encrypted with the wrong key." The examiner respectfully disagrees.

Shrader et al. teach a method and system for assisting a user in verifying a cast ballot recorded (saved, stored, executed, etc.) in a system (server) comprising (Abstract; Paragraphs 0050-0053; 0060-0063; Figures 4-8) forming (generating, creating, signing, encrypting, etc.) a digital signature of a cast ballot using the private key of a system (server; "The voting tabulator *signs, encrypts and sends the encrypted electronic ballot* to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and signed with the *validator's private key*; Paragraph 0063; Figures 7-8, Element 72); associating (storing, linking, relating, etc.) the cast ballot, the voter's digital signature of the ballot with a ballot number (vote serial number, unique number/unique identifier, etc.; validating ballot request; Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71) and forming a message (confirmation, string, receipt, acknowledgement, token, etc.) comprising a system's digital signature of the ballot and the ballot number (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8).

Specifically regarding Applicant's argument that the prior art of record fails to teach or suggest "the inclusion of the digital signature of the cast ballot using the server's private key as an element of the association called for in Claim 31" the examiner respectfully disagrees.

Cranor et al. teach a method and system for assisting a user in verifying (validating, authenticating, certifying, etc.) a cast ballot (vote) recorded (saved, stored, etc.) in a server (system) the method/system comprising forming (generating, creating, signing, encrypting, etc.) a digital signature of the ballot using the private key of a system (Paragraph 2, Page 5).

Shrader et al. teach a method and system for assisting a user in verifying a cast ballot recorded (saved, stored, executed, etc.) in a system (server) comprising (Abstract; Paragraphs 0050-0053; 0060-0063; Figures 4-8) forming (generating, creating, signing, encrypting, etc.) a digital signature of a cast ballot using the private key of a system (server; "The voting tabulator signs, encrypts and sends the encrypted electronic ballot to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and singed with the validator's private key; Paragraph 0063; Figures 7-8, Element 72).

Specifically regarding Applicant's argument that the prior art of record fails to teach or suggest assisting a user in verifying their vote, the examiner respectfully disagrees.

As an initial matter it is noted that the methods steps, as currently claimed, do not positively recite who or what entity is performing the various steps nor do positively recite that the "a user" actually receives and verifies their own cast ballot as argued.

For example, Claim 1 merely recites "making a confirmation token available to *a user*" (emphasis added) however the claim does not positively recite (what entity makes the token available to a user) nor does the invention as claimed positively recite which user (the "a user" recited in the preamble or another user of the system) the token is made available to nor does the invention as claimed positively recite what entity (the "a user" in the preamble or some other entity/participant) actually retrieves/receives the now available confirmation token nor does the invention as claimed positively recite what entity performs the comparison to determine that the cast ballot is verified (the "a user" of the preamble or another method participant/entity).

Further it is noted that the features upon which applicant relies (i.e., users verifying their own cast ballots) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Further it is noted that the recitation in the preamble merely represents non-functional descriptive material wherein the intended use of the he intended use of the of method for securely voting over a network, i.e. assisting users in validating cast ballots

(individual verifiability, merely recites non-functional descriptive material and are not functionally involved in the steps recited nor do they alter the recited structural elements. The recited method steps would be performed the same regardless of the intended use of the of method for securely voting over a network. Further, the structural elements remain the same regardless of the intended use of the of method for securely voting over a network. Thus, this descriptive material will not distinguish the claimed invention from the prior art in terms of patentability, *see In re Gulack, 703 F.2d 1381, 1385, 217 USPQ 401, 404 (Fed. Cir. 1983); In re Lowry, 32 F.3d 1579, 32 USPQ2d 1031 (Fed. Cir. 1994); MPEP 2106.*

Further it is noted that the recitation "assisting users in verifying a cast ballot" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Additionally enabling voters (users) to individually verify that their cast ballot was cast correctly/accurately, commonly referred to as individual verifiability, is old and very well known as is encrypting cast ballots, wherein the cast ballots contain a votes serial

number for unique identification, and the vote(s), as evidenced by at least the following references:

- Shrader et al. teach a system and method for assisting users in verifying their cast ballot (individual verifiability, Paragraph 0026; confirmation token, Paragraph 0063).
- Cranor et al. teach a system and method for voting securely over a network comprising assisting users in verifying their vote (individual verifiability: Last Paragraph, Page 13; Paragraphs 1-2, Page 12, "receipt #", Figure 1, Paragraphs 3-4, Page 8, db index, Paragraph 1, Page 11) and providing a confirmation token to the user (receipt; Figure 1, Paragraph 2, Page 12, Paragraph 3, Page 8).

  > Verifiability. A system is verifiable if voters can independently verify that their votes have been counted correctly.
  >
  > The most verifiable systems *allow all voters to verify their votes* and correct any mistakes they might find without sacrificing privacy. Less verifiable systems might allow mistakes to be pointed out, but not corrected or might allow verification of the process by party representatives but not by individual voters. (Paragraph 1-2, Page 4)

- Reardon US 6,968,999: Column 5 Lines 55-68, Fig 2 E 23, 24; Column 3 Lines 23-38, Column 5 Lines 63-68, Fig 2 Elements 23,2 4
- Chung US 7,036,730: Column 7 Lines 8-23, Column 8 Lines 37-55; "voting session identifier", Column 2 Lines 60-68, Column 3, Lines 8-30, Column 5 Lines 8-15, 56-58; Column 10 Lines 35-45, Figure 4c

- VoteHere.net - Web Pages Internet Voting Primer White Paper (August 2000) – teaches individual verifiability and encrypting cast ballots:

> Individually Verifiable Election Systems
>
> Current individually verifiable systems are efficient and flexible. They allow arbitrary ballot types (yes/no, d-of-N options, write-ins). However, the most significant disadvantage of these systems is that the voter is responsible for insuring that his vote was accounted for in the final election tally. This individual verifiability property is highly impractical for civic elections no independent observer can verify the election.
>
> The *privacy of individually verifiable election systems [FOO92, PIK93, Cra96, Sch95] comes from blind signatures*. Blind signatures [Cha81] are a class of digital signatures that allow a document to be signed without revealing its contents. An often used analogy is that of placing a document and a sheet of carbon paper inside an envelope. If somebody signs the outside of the envelope, the carbon paper transfers the signature to the document on the inside of the envelope. The signature remains on the document when removed from the envelope.
>
> Typically, *a voter blinds and digitally signs his voted ballot* and submits it to a verifying authority. The *voted ballot also contains a unique serial number* generated by the voter. Once the *voter submits the blinded vote* to the verifier, the verifier checks the voter's digital signature and voter eligibility. If all criteria are

met, the verifier checks the voter off the voter roles, countersigns the voted ballot, and sends the blinded, *countersigned ballot back to the voter.*

The voter removes the blinding encryption layer revealing the verifying authority's signature. Now that all voter specific information is removed from the ballot, the voter submits it to the tallying authority through an anonymous channel. An anonymous communications (e.g., onion routing) channel protects the message with multiple layers of encryption using randomly selected intermediate points (see [SGR] for a discussion of onion routing). The tallying authority authenticates the verifying authority's digital signature and adds the results to the tally.

....

A possible counter to these attacks is a bit commitment (i.e., *a ballot serial number*) on the authority-signed ballot returned to the voter [FOO92, PIK93]. *The voter*, then, can detect attacks where the *voted ballot or ballot serial number* have been modified *by checking to make sure that his ballot number is present among the published ballots and that it contains the correct vote.* Note that the voter must also make sure that his signed ballot request is present; otherwise, the authority could have deleted it to offset the deletion of someone else's ballot. If something is amiss, the voter can dispute the election results. Again, this is weak protection because a significant number of voters must perform the verification. (emphasis added, Page 9)

- Varadharajan et al., Anonymous Secure E-Voting over a Network teach a system and method for securely voting over a network wherein voters cast and encrypt their cast ballots, containing their vote/ballot choices (Column 1, Last Paragraph, Page 4; Column 2, Paragraph 1, Last Paragraph, Page 4; Column 1, Paragraph 1, Step 2, Page 5). Varadharajan et al. further teach that there are two old and well known techniques for protecting the privacy of voters namely non-anonymous (hides the contents of votes) and anonymous (hides identify of voters and leaves content of votes in plaintext/clear; Column 1, Last Paragraph, Page 1; Column 2, Paragraph 1, Page 1).

Specification

3. The amendment filed April 6, 2007 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: Paragraphs 0018 and 0023.

Specifically the extensive revisions to Paragraph 0018, the removal of Paragraph 0023 in its entirety and the addition of a new figure, Figure 5 removes from the specifications pertinent sections which disclose when a vote serial number is assigned to a ballot, which is one of the Applicant's key arguments (Remarks: Last Paragraph, Page 11).

Newly amended Paragraph 0018 teaches associating a vote serial number with a ballot *after* it has been cast (cast ballot), however the originally filed specification does not disclose this feature and in fact discloses the *opposite*, associating a vote serial number with a ballot *prior* to the ballot being cast by a voter.

More specifically, Paragraph 0018, as originally filed, discloses that the Vote Serial Number (VSN) is assigned to the ballot *prior to the ballot being cast,* see below (emphasis added), as opposed to being assigned after the ballot is cast as the Applicant's currently argue.

[0018] In accordance with one aspect of the invention, there is provided *a method of securely voting over a network*, which can be a local area network, or a wide area network such as the global computer network known as the Internet. The method involves **delivering an**

electronic ballot from a server with a vote serial number on the ballot, to an individual at a terminal over a connection secured using both the server's and the voter's private keys. Thereafter, the ballot is filled in with the voter's choices, which are digitally signed using the voter's private key. The voter's ballot choices, bearing the voter's electronic signature, and the vote serial number is then delivered to the server. A data element is then created from the individual's digital signature of the ballot choices, the server's digital signature of the voter's ballot choices (created using the server's private key) and the vote serial number to allow recording of the subset of the ballot in a data store at the server, and retaining the ballot information as a vote. This data element is then digitally signed using the server's private key to ensure its integrity and authenticity.

Additionally the newly revised Paragraph 0018 introduces the "individually verify" steps/processes wherein the concept of individual verification was not explicitly disclosed in the originally filed specification.

Paragraph 0023, as originally filed, also discloses that the Vote Serial Number (VSN) is assigned to the ballot *prior to the ballot being cast,* see below (emphasis added), as opposed to being assigned *after* the ballot is cast as the Applicant's currently argue.

> [0023] In an alternative aspect, there is described a system for conducting *secure voting over a network*, for example, the global computer network known as the Internet, or on a local area network. The system includes a server having a data store associated therewith. The server is configured for connection to the network for communicating with terminals connected to the network. The server is further configured for **delivering**

an electronic ballot having the vote serial number on the ballot, to an individual at a terminal connected to the network, and the ballot being configured for being filled in by the individual, and for having a subset thereof delivered to the server with the individual's electronic signature, and the vote serial number thereon.

Applicant is required to cancel the new matter in the reply to this Office Action.

Further it is noted that this lack of support for the alleged patentable element(s) of the claimed invention was also discussed in detail during the October 5, 2006 and November 2, 2006 interviews with the Applicant's representative; an excerpt from the November 2nd interview is provided below for the Applicant's convenience (emphasis added).

Applicant's representative and examiner discussed several features that Mr. Dimino and Mr. Corrado felt distinguished the instant application, per discussions during the October 5, 2006 interview and applicant's remarks filed October 10, 2006, namely individual verifiability and the assignment of a vote serial number. The examiner performed a quick review of the prior art to demonstrate *why these features were unlikely to distinguish the instant application over the prior art.* Note: This is not a complete search, just an initial review to show that the features are well known.

References teaching Individual Verifiability and Vote Serial Number:

- Cranor et al., Design and Implementation of a Practical Security Conscious Electronic Polling System (1996), P 1-2, Pg 12, "receipt #", Fig 1, P3-4, Page 8, db index, P1, Pg 11
- VoteHere.net We Pages (2000) P5, Pg 17, P3,6, Pg 9, Pg 13
- Reardon US 6,968,999: C5 L55-68, Fig 2 E 23, 24; C3 L23-38, C5 L63-68, Fig 2 E23,24
- Chung US 7,036,730: C7 L8-23, C8 L37-55, "voting session identifier", C2 L60-68, C3, L8-30, C5 L8-15, 56-58; C10 L35-45, Fig 4c

Applicant's representative and examiner further discussed that in the remarks filed October 10 *several of the features argued are not positively recited in the body of the claims*, specifically that the VSN has no relationship with the voter, voters validating their own ballot and that the verification message does not contain the actual votes from the ballot.

Applicant's representative and examiner discussed Paragraph 0018 of the specification which indicates that the *vote serial number is applied to the ballot prior to it being cast by the voter*, whereby the examiner was unable to find support for the applicant's suggestion that the vote serial number was only applied after the voter cast their ballot - "The method involves delivering an electronic ballot from a server with a vote serial number on the ballot, to an individual at a terminal over a connection secured using both the server's and the voter's private keys. Thereafter, the ballot is filled in with

the voter's choices, which are digitally signed using the voter's private key. The voter's ballot choices, bearing the voter's electronic signature, and the vote serial number is then delivered to the server."

Drawings

4. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because Figure 3B contains a grammatical error. Element 19 contains a "Jron" element instead of the intended and originally filed "Jrun" element. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Objections

5. Claims 31-32 are objected to because of the following informalities: claim 31 contains a grammatical error at the end of line 13, line 13 should read "receiving a confirmation token;". Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 29-30 and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claims 29 and 33 Shrader et al. teach a method and system for assisting a user in verifying a cast ballot recorded (saved, stored, executed, etc.) in a system (server) comprising (Abstract; Paragraphs 0050-0053; 0060-0063; Figures 4-8):

- forming (generating, creating, signing, encrypting, etc.) a digital signature of a cast ballot using the private key of a system (server; "The voting tabulator *signs, encrypts and sends the encrypted electronic ballot* to the voting mediator 72 in a message that is encrypted with the voting mediator's public key and signed with the *validator's private key*; Paragraph 0063; Figures 7-8, Element 72);

- associating (storing, linking, relating, etc.) the cast ballot, the voter's digital signature of the ballot with a ballot number (vote serial number, unique number/unique identifier, etc.; validating ballot request; Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71);

- forming a message (confirmation, string, receipt, acknowledgement, token, etc.) comprising a system's digital signature of the ballot and the ballot number (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- making the message available (verification message exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8);

- receiving the message (verification message(s) exchanged between tabulator to mediator; Paragraphs 0061, 0063; Figures 7-8, Elements 72-74);

- extracting (decrypting, stripping, de-signing, deciphering, etc.) the ballot number and the system's digital signature from the message (verification message(s) exchanged between tabulator to mediator; Paragraph 0063; Figures 7-8, Elements 73-75);

- for vote serial number comparing the system's digital signature of the ballot received to the system's digital signature of the ballot (Paragraphs 0061-0063; Figures 7-8); and

- if the comparison shows equivalency (match, consistency, equality, etc.) determining that cast ballot (message, token, etc.) is verified (valid, authentic, genuine, unaltered, secure, etc.; Paragraphs 0061, 0063; Figures 7-8).

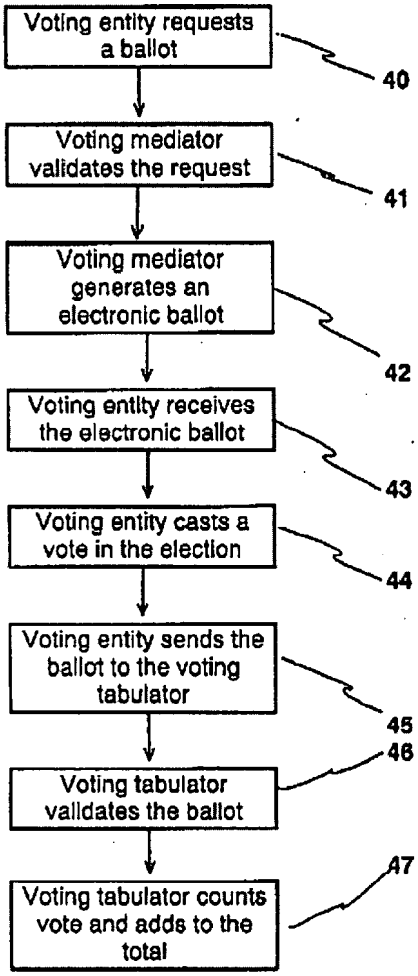
Voting entity requests a ballot
40
Voting mediator validates the request
41
Voting mediator generates an electronic ballot
42
Voting entity receives the electronic ballot
43
Voting entity casts a vote in the election
44
Voting entity sends the ballot to the voting tabulator
45
Voting tabulator validates the ballot
46
Voting tabulator counts vote and adds to the total
47

FIG. 4

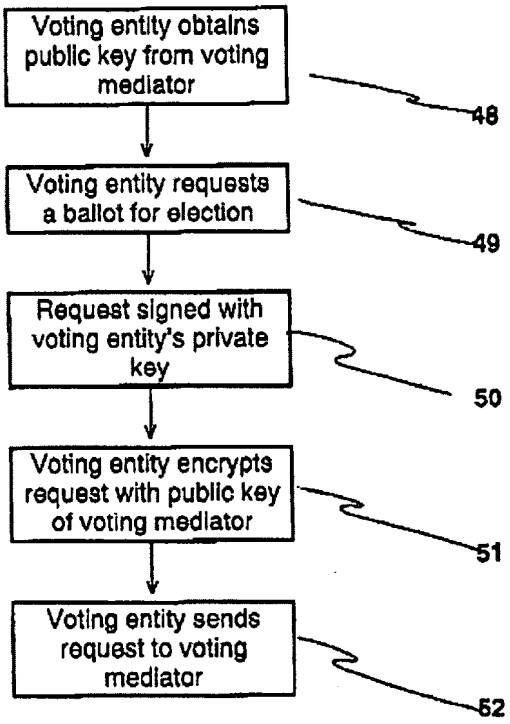
Voting entity obtains public key from voting mediator
48
Voting entity requests a ballot for election
49
Request signed with voting entity's private key
50
Voting entity encrypts request with public key of voting mediator
51
Voting entity sends request to voting mediator
52

FIG. 5

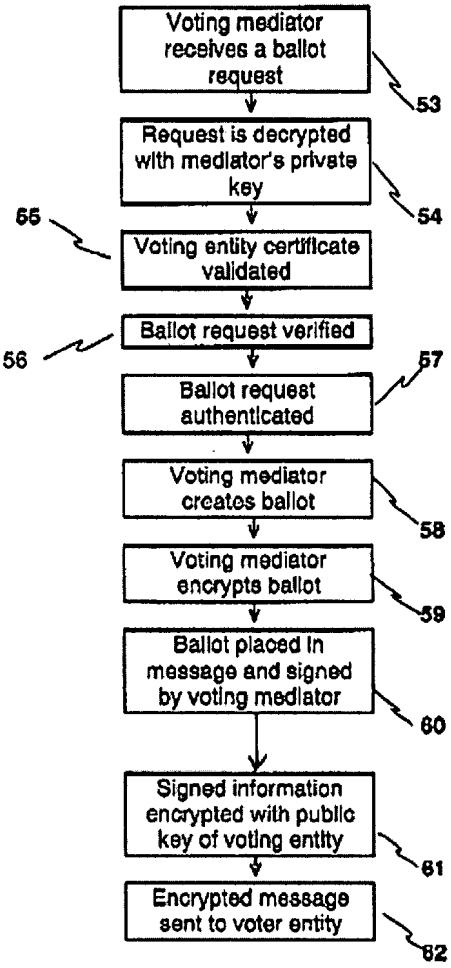
Voting mediator receives a ballot request
53
Request is decrypted with mediator's private key
54
55
Voting entity certificate validated
Ballot request verified
56
57
Ballot request authenticated
Voting mediator creates ballot
58
Voting mediator encrypts ballot
59
Ballot placed in message and signed by voting mediator
60
Signed information encrypted with public key of voting entity
61
Encrypted message sent to voter entity
62

FIG. 6

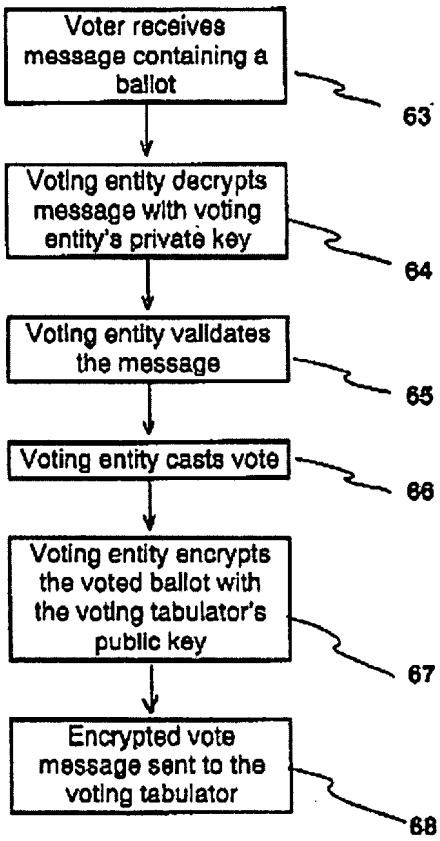
Voter receives message containing a ballot
63
Voting entity decrypts message with voting entity's private key
64
Voting entity validates the message
65
Voting entity casts vote
66
Voting entity encrypts the voted ballot with the voting tabulator's public key
67
Encrypted vote message sent to the voting tabulator
68

FIG. 7

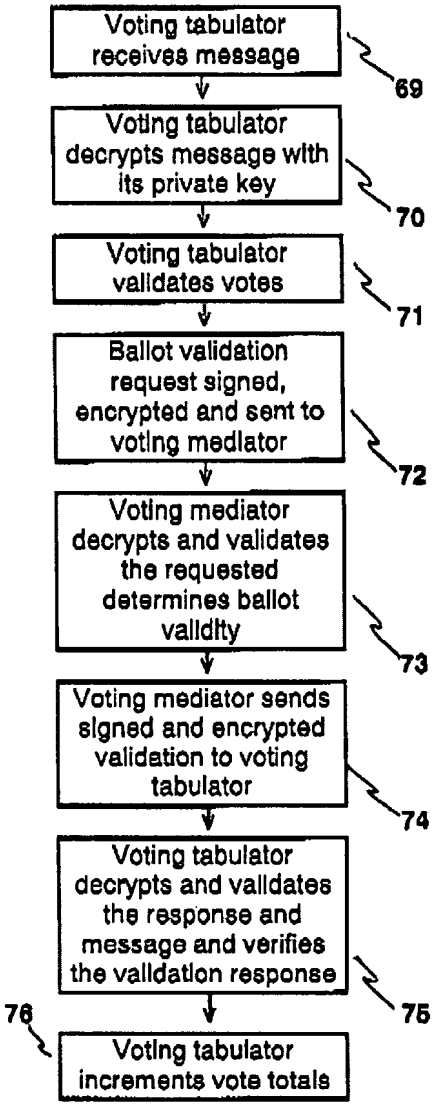

FIG. 8

Regarding Claim 30 Shrader et al. teach a method and system for assisting a user in verifying a ballot recorded in a system wherein the message (confirmation token, received token) further comprises the system's digital signature of the ballot and ballot number (aggregation; Paragraphs 0060-0062; Figure 2, Certificate No.); and wherein the method further comprises the steps of:

- extracting a digital signature of the ballot and ballot number (aggregation) from the message (received token; Paragraphs 0060, 0061, 0063; Figures 6-8); and

- the cast ballot is verified only upon the additional condition that the server's received digital signature of the aggregation is equivalent to the server's digital signature of the aggregation (Paragraphs 0061, 0063; Figures 6-8; Elements 67-75).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cranor et al., Design and Implementation of a Practical Security-Conscious Electronic Polling System (1996) in view of Shrader et al., U.S. Patent Publication No. 2002/0077887.

Regarding Claim 31 Cranor et al. teach a method and system for assisting a user in verifying (validating, authenticating, certifying, etc.) a cast ballot (vote) recorded (saved, stored, etc.) in a server (system) the method/system comprising (Abstract; Figures 1,3):

- receiving, in a system (server, computer, terminal, device, etc.), at least one set of a cast ballot and a voter's digital signature of the ballot (Paragraph 2, Page 5);

- forming (generating, creating, signing, encrypting, etc.) a digital signature of the ballot using the private key of a system (Paragraph 2, Page 5);

- associating (storing, linking, relating, etc.) the cast ballot, voter's digital signature of the ballot and the voter's identification number (Paragraphs 3-4, Page 7);

- forming a message (confirmation token, string, receipt, acknowledgement, etc.) comprising system's digital signature of the cast ballot, the voter's digital signature of the cast ballot, and the system's digital signature of the aggregation of the cast ballot, the voter's digital signature of the ballot and the system's digital signature of the ballot ("validator", "tallier", "validation certificate", "receipt"; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- making the message (token, string, etc.) available to a user (entity, voter, system, subsystem, third party, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- receiving the messages (confirmation, token, verification, acknowledgement, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1);

- extracting (decrypting, stripping, etc.) *at least one of the following* from the message Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

  - voter's digital signature of the ballot; ***or***

  - system's digital signature of the ballot; ***or***

  - system's digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation);

- for extracted ballot number and the corresponding ballot number comparing *at least one of the following* (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1):

- voter's digital signature of the ballot extracted from the message and voter's digital signature of the ballot; ***or***
- system's digital signature of the ballot extracted from the message and system's digital signature of the ballot, **or**
- system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation) extracted from the message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, ballot number (aggregation); and

- if the comparison shows equivalency (match, consistency, equality, etc.) determining that the cast ballot is verified (valid, authentic, genuine, unaltered, accepted, counted, etc.; Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8; Figure 1).

Cranor et al. further teaches individual verifiability (Paragraphs 1-2, Page 12) as well as a unique vote/ballot identifier (receipt number/#; Figure 1, Pages 3-4; Page 8; db index, Paragraph 1, Page 11).

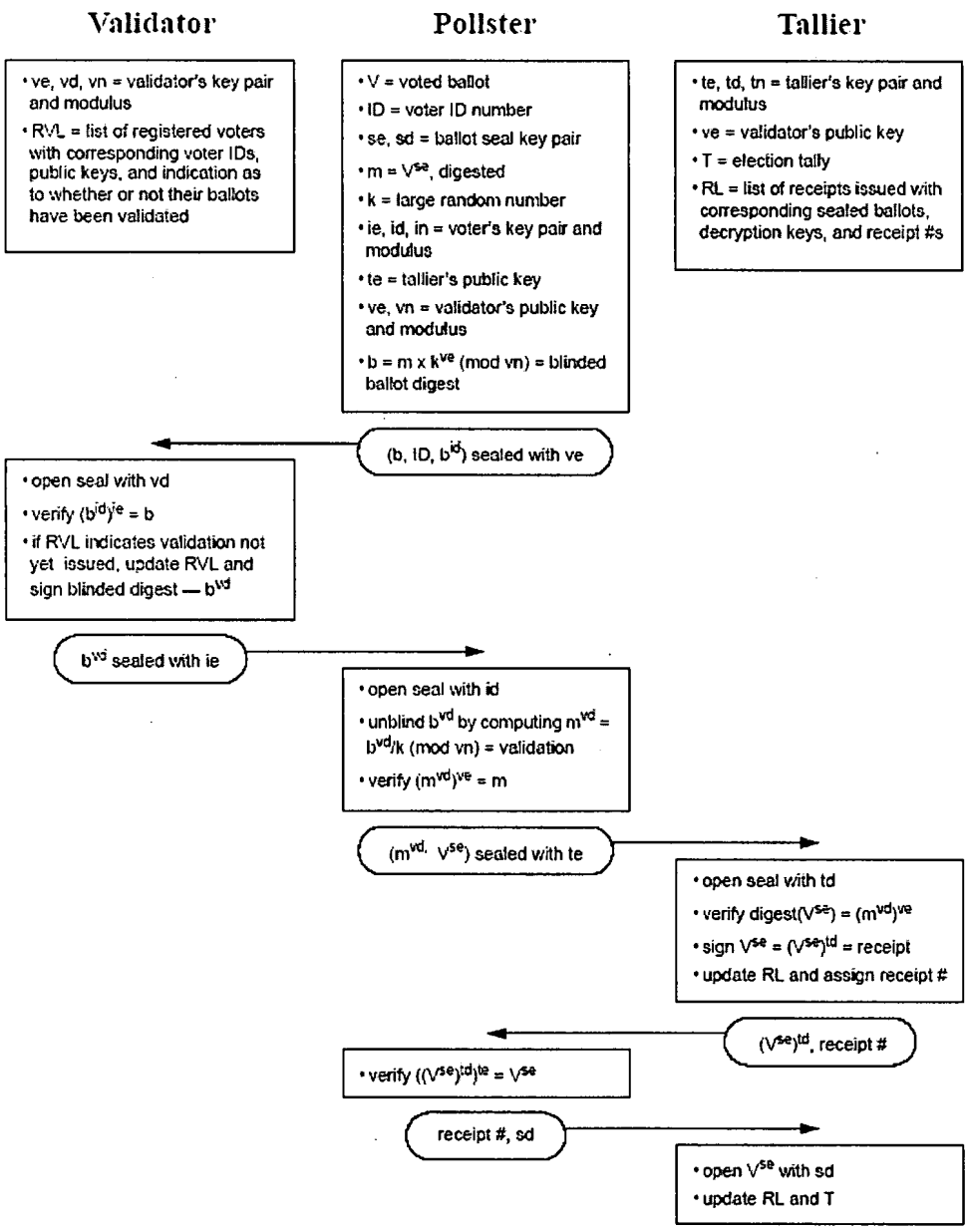

Figure 1: Blind Signature Protocol Overview

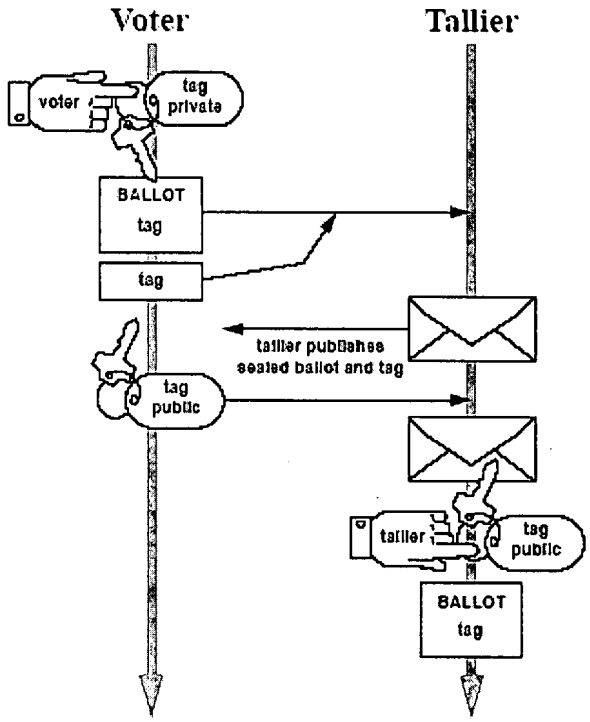

Figure 3: Phase 2 of the Two Agency Protocol

Cranor et al. teaches a system and method for voting securely over a network comprising *associating at least two unique identifiers with ballots cast by voters* wherein the unique identifiers (vote serial numbers) are generated and associated with the cast ballot only *after* the voters casts their ballot containing their choices (receipt number: Paragraphs 3-4, Page 8; Figure 1; index number for uniquely identifying, accessing and storing cast ballots in a database, Paragraph 4, Page 8)

Our tallier computes a 16-byte digest of *each encrypted ballot received* and uses it *to index the encrypted ballots and receipts*. A hash table could be added for greater efficiency in *looking up encrypted ballots*. This modification is probably necessary to accommodate large-scale elections. (emphasis added, Paragraph 4, Page 8)

While the use of unique identifiers for (paper and/or electronic) ballots is a common practice Cranor et al. does not expressly teach that the cast ballot contains a vote serial number as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID, certificate no.) in an analogous art of secure electronic voting/balloting over a network for the purposes of ensuring voters only cast their ballot once (Paragraph 0061; Figures 2, 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only vote once (Shrader et al.: Paragraph 0063).

Regarding Claim 32 Cranor et al. teach a method and system for verifying a cast ballot recorded in a system further comprising if the comparison shows equivalence between the system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot, the system's digital signature of the ballot, extracted from the

message and system's digital signature of the ballot, digital signature of the voter's digital signature of the ballot and the system's digital signature of the ballot (aggregation) determining that the message (token) has not been modified (altered, disturbed, edited, etc.) since its formation (Paragraph 2, Page 5; Last Paragraph, Page 7; Paragraphs 1-4, Page 8).

Cranor et al. does not expressly teach that ballots further comprise vote serial numbers as claimed.

Shrader et al. teach that ballots comprise a vote serial number (unique ballot ID) in an analogous art of secure electronic voting/balloting for the purposes of ensuring voters only cast their ballot once (Paragraph 0061; Figures 5-6, Elements 57, 58; validating/authenticating cast ballot; Paragraph 0063; Figure 8, Element 71).

It would have been obvious to one skilled in the art at the time of the invention that the system and method for verifying a cast ballot recorded on a system (server) as taught by Cranor et al. would have benefited from including in the ballot a unique ballot identifier (vote serial number) in view of the teachings of Shrader et al.; the resultant system/method providing an additional mechanism for ensuring that valid voters only cast their ballot once (Shrader et al.: Paragraph 0063).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Green et al., WO 01/22200 A2, teach a system and method for voting securely over a network (Internet) comprising voters casting and encrypting (signing) their cast ballots, providing a cast ballot receipt (confirmation token) to the voter, and voter/individual verifiability.

- Borrell et al., An implementable secure voting scheme (1996), teach a system and method for secure voting wherein all communications between voters and the system are encrypted using well known cryptosystems and that the system allows verification of the cast ballot by individual voters.

- Dechert, The Voter Certified Ballot (2001), teaches a system and method assisting voters to verifying that their cast ballot was properly recorded and counted.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott L. Jarrett whose telephone number is (571) 272-7033. The examiner can normally be reached on Monday-Friday, 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hafiz Tariq can be reached on (571) 272-6729. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Scott Jarrett
Asst. Examiner
June 6, 2007

TARIQ R. HAFIZ
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600